Amendment to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

1. (Currently Amended) A system for interdicting unauthorized copying in a decentralized network comprising:

one or more first computers having a plurality of software agents masquerading as nodes in a decentralized network; and

one or more second computers in communication with the one or more first computers but no other nodes in the decentralized network, the one or more second computers having a query matcher that receives search results from the plurality of software agents, and reports matches of the search results with protected files back to the plurality of software agents so that the software agents can interdict unauthorized copying of the protected files in the decentralized network.

2. (Previously Presented) The system according to claim 1, wherein the plurality of software agents communicate with the decentralized network through assigned ports.

3. (Previously Presented) The system according to claim 2, wherein the assigned ports have corresponding IP addresses that change in a manner so as to deter detection of the plurality of software agents as unauthorized masqueraders of nodes in the decentralized network.

4. (Previously Presented) The system according to claim 2, wherein the number and geographical locations of the one or more first computers is determined by the number and geographical distribution of nodes in the decentralized network.

5. (Previously Presented) The system according to claim 1, wherein the one or more second computers has a database including metadata for the protected files.

6. (Previously Presented) The system according to claim 1, wherein the one or more second computers has a central coordinating authority coordinating activities of the plurality of software agents so as to interdict unauthorized copying in the decentralized network.

7. (Original) The system according to claim 6, wherein the central coordinating authority sends instructions to the plurality of software agents specifying actions to be taken when the plurality of software agents receive matches of the search results with protected files back from the query matcher.

8. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to generate modified search results by deleting at least a subset of references corresponding to the matches of the search results, and forward the modified search results through the decentralized network.

9. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to generate modified search results by modifying at least a subset of references corresponding to the matches of the search results so as to point to one or more IP addresses that are invalid, and forward the modified search results through the decentralized network.

10. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to generate modified search results by modifying at least a subset of references corresponding to the matches of the search results so as to point to one or more IP addresses of nodes that do not have copies of the subset of references, and forward the modified search results through the decentralized network.

11. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to generate modified search results by modifying at least a subset of references corresponding to the matches of the search results so as to point to one or more IP addresses of nodes that are not connected to the decentralized network, and forward the modified search results through the decentralized network.

12. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to generate modified search results by modifying at least a subset of references corresponding to the matches of the search results so as to point to alternative files, and forward the modified search results through the decentralized network.

13. (Original) The system according to claim 12, wherein the alternative files include at least one randomly selected file residing on a node upon which one of the matches of the search results resides.

14. (Original) The system according to claim 12, wherein the alternative files include at least one decoy file residing on a host node controlled by the central coordinating authority.

15. (Original) The system according to claim 12, wherein the alternative files include at least one randomly selected file residing on a host node controlled by the central coordinating authority.

16. (Original) The system according to claim 12, wherein the alternative files include at least one rights-managed version of the matches.

17. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to send an alternative file to a client node when a request for a protected file is received from the client node.

18. (Original) The system according to claim 17, wherein the alternative file is a decoy.

19. (Original) The system according to claim 18, wherein the decoy is an audio file containing white noise.

20. (Original) The system according to claim 18, wherein the decoy is a video file containing white noise.

21. (Original) The system according to claim 18, wherein the decoy is an application containing a NOP executable that terminates the application when executed.

22. (Original) The system according to claim 18, wherein the decoy is an image file containing snow.

23. (Original) The system according to claim 18, wherein the decoy is a document with blank contents.

24. (Original) The system according to claim 18, wherein the decoy contains an anti-piracy message.

25. (Original) The system according to claim 17, wherein the alternative file is a rights managed version of the protected file.

26. (Withdrawn) The system according to claim 17, wherein the instructions sent by the central coordinating authority include an instruction to transmit the alternative file such that the transmission rate slows down during the transmission.

27. (Withdrawn) The system according to claim 17, wherein the instructions sent by the central coordinating authority include an instruction to transmit the alternative

file such that the transmission terminates automatically after most, but not all of the alternative file has been downloaded.

28. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to modify at least one reference corresponding to a match in the search results so as to point to a non-existent file along with a reported hash value that does not correspond to any file in the decentralized network instead of the at least one reference.

29. (Original) The system according to claim 7, wherein the instructions sent by the central coordinating authority include an instruction to modify a reference corresponding to a match in the search results so as to point to a spoof file instead of the reference and report a hash value matching that of the reference even though the contents of the spoof file do not exactly match that of the reference.

30. (Original) The system according to claim 1, wherein the decentralized network comprises:

a plurality of nodes; and

a plurality of supernodes individually having higher resources than each of the plurality of nodes so that a search string initiated from one of the plurality of nodes is first routed to one of the plurality of supernodes.

31. (Original) The system according to claim 30, wherein the plurality of software agents inform their respective supernodes that they have copies of protected files and claim node attributes so that the plurality of software agents will be selected as top matches by their respective supernodes for search strings indicating the protected files.

32. (Original) The system according to claim 30, wherein the plurality of software agents inform the decentralized network that they are supernodes.

33. (Original) The system according to claim 30, wherein the plurality of software agents report to the decentralized network that they possess attributes that qualify them as supernodes under the protocol of the decentralized network.

34. (Currently Amended) A method for interdicting unauthorized copying in a decentralized network, comprising:

infiltrating a decentralized network with a plurality of software agents residing on one or more first computers and masquerading as nodes of the decentralized network so as to intercept communications related to search queries;

transmitting information of the intercepted communications to one or more second computers that do not communicate with or intercept communications of any other nodes ~~external~~ of the decentralized network so that a query matcher residing on the one or more second computers identifies references to protected files in the communications; and

transmitting information of identified references from the one or more second computers [[back]] to corresponding of the one or more first computers for interdicting unauthorized copying of the protected files with respect to the communications.

35. (Original) The method according to claim 34, wherein the decentralized network is an hierarchical network with supernodes and regular nodes, and the plurality of software agents masquerade as regular nodes that inform their respective supernodes that they have copies of protected files and claim node attributes so that the plurality of software agents will be selected as top matches by their respective supernodes for search strings indicating the protected files.

36. (Original) The method according to claim 34, wherein the decentralized network is an hierarchical network with supernodes and regular nodes, and the plurality of software agents inform the decentralized network that they are supernodes according to the protocol of the decentralized network.

37. (Original) The method according to claim 34, wherein the decentralized network is an hierarchical network with supernodes and regular nodes, and the plurality of software agents report to the decentralized network that they possess attributes that qualify them as supernodes under the protocol of the decentralized network.

38. (Original) The method according to claim 34, wherein the communications are search results, and the interdicting of unauthorized copying comprises: generating modified search results by deleting at least a subset of references corresponding to the protected files in the search results, and forwarding the modified search results through the decentralized network.

39. (Original) The method according to claim 34, wherein the communications are search results, and the interdicting of unauthorized copying comprises: generating modified search results by modifying at least a subset of references corresponding to the protected files in the search results to point to one or more invalid IP addresses, and forwarding the modified search results through the decentralized network.

40. (Original) The method according to claim 34, wherein the communications are search results, and the interdicting of unauthorized copying comprises: generating modified search results by modifying at least a subset of references corresponding to the protected files in the search results to point to one or more IP addresses that do not host the subset of references, and forwarding the modified search results through the decentralized network.

41. (Original) The method according to claim 34, wherein the communications are search results, and the interdicting of unauthorized copying comprises: generating modified search results by modifying at least a subset of references corresponding to the protected files in the search results to point to one or more IP addresses that are not connected to the decentralized network, and forwarding the modified search results through the decentralized network.

42. (Original) The method according to claim 34, wherein the communications are search results, and the interdicting of unauthorized copying comprises: generating modified search results by modifying at least a subset of references corresponding to the protected files in the search results to point to alternative files, and forwarding the modified search results through the decentralized network.

43. (Original) The method according to claim 42, wherein the alternative files include at least one synthesized decoy file.

44. (Original) The method according to claim 42, wherein the alternative files include at least one rights-managed version of one of the protected files referenced in the search results.

45. (Original) The method according to claim 34, wherein one of the communications is a request from a client node to one of the plurality of software agents for a copy of a protected file, and further comprising: sending an alternative file to the client node in lieu of the copy of the protected file.

46. (Original) The method according to claim 45, wherein the alternative file is a synthesized decoy file.

47. (Original) The method according to claim 46, further comprising: synthesizing the decoy file by filling the decoy file with white noise.

48. (Original) The method according to claim 46, further comprising: synthesizing the decoy file by filling the contents of the decoy file with an anti-piracy message.

49. (Original) The method according to claim 46, wherein the protected file is an application program, and further comprising: synthesizing the decoy file by including a NOP executable that terminates when executed.

50. (Original) The method according to claim 45, wherein the alternative file is a rights-managed version of the protected file.

51. (Withdrawn) The method according to claim 45, wherein the sending an alternative file comprises: transmitting the alternative file at a transmission rate that slows down during the transmission.

52. (Withdrawn) The method according to claim 45, wherein the sending an alternative file comprises: transmitting the alternative file in a manner such that the transmission terminates automatically after most, but not all of the alternative file has been downloaded.

53. (Original) The method according to claim 34, wherein one of the communications is search results, and the interdicting of unauthorized copying comprises: generating modified search results by providing a pointer to a non-existent file instead of another pointer to a reference in the search results that matches a protected file, and forwarding the modified search results through the decentralized network.

54. (Original) The method according to claim 53, wherein a reported hash value that does not match any file in the decentralized network is provided along with the pointer to the non-existent file.

55. (Original) The method according to claim 34, wherein one of the communications is search results, and the interdicting of unauthorized copying comprises: generating modified search results by replacing a pointer to a reference in the search results that matches a protected file with another pointer to a spoof file along with a hash value matching that of the reference, and forwarding the modified search results through the decentralized network.

56. (Original) The method according to claim 34, wherein one of the communications is a request to one of the plurality of software agents from a client node for at least a segment of a protected file, and the interdicting of unauthorized copying comprises: transmitting data to the client node in response to the request so that a corrupted file is detected upon completion of downloading of the protected file to the client node.

Claims 57-70 (Cancelled).

71. (New) The system according to claim 1, wherein the one or more first computers communicate with the one or more second computers over a private network.

72. (New) The method according to claim 34, wherein the one or more first computers communicate with the one or more second computers over a private network.

73. (New) A method for interdicting unauthorized copying of a protected file in a decentralized network comprising:

receiving search results from a node responding to a search initiated by a search initiating node in a decentralized network;

modifying the search results so as to interdict unauthorized copying of a protected file; and

forwarding the modified search results through the decentralized network to the search initiating node.

74. (New) The method according to claim 73, wherein the modifying of the search results comprises: deleting at least one reference corresponding to the protected file in the search results.

75. (New) The method according to claim 73, wherein the modifying of the search results comprises: modifying at least one reference corresponding to the protected file in the search results so as to point to an invalid IP address.

76. (New) The method according to claim 73, wherein the modifying of the search results comprises: modifying at least one reference corresponding to the protected file in the search results so as to point to an IP address that does not host the reference.

77. (New) The method according to claim 73, wherein the modifying of the search results comprises: modifying at least one reference corresponding to the protected file in the search results so as to point to an IP address that is not connected to the decentralized network.

78. (New) The method according to claim 73, wherein the modifying of the search results comprises: modifying at least one reference corresponding to the protected file in the search results to point to an alternative file.

79. (New) The method according to claim 78, wherein the alternative file comprises a decoy file.

80. (New) The method according to claim 78, wherein the alternative file comprises a rights-managed version of the protected file.